Marine Corps University / Command and Staff College
The Electives Program

Cyber Warfare
Bibliography: Command and Staff College
Marine Corps University, Quantico, VA
Dr. Matthew J. Flynn 1/15

This bibliography is compiled from the scholarly literature listed below. The topics covered reflect the priorities of Command and Staff College. mjf

Academic Journals

Contemporary Security Policy (Routledge)
Foreign Affairs
International Affairs (UK)
Journal of International Affairs (Columbia)
International Security (MIT)
Journal of Strategic Studies (Routledge)
Security Studies (Routledge)
The Washington Quarterly
World Politics (Cambridge)

Within PME Circles

Joint Force Quarterly
Strategic Studies Quarterly
Parameters
Military Review
Small Wars Journal

Defining Cyber Warfare

"Cyber Roundtable," *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013): 101-142.

1. John Stone, "Cyber War Will Take Place."
2. Gary McGraw, "Cyber War is Inevitable (Unless We Build in Security)."
3. Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment."
4. Timothy J. Junio, "How Probable is Cyber War?: Bringing IR Theory Back in to the Cyber Conflict Debate."
5. Adam P. Liff, "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio."
6. Thomas Rid, "More Attacks, Less Violence."

Andress, Jason and Winterfeld, Steve. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham, MA: Syngress, 2011.

Brickey, John. "The Case for Cyber." *Small Wars Journal*, Sept 13, 2012. (9)

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins Publishers, 2010. Pp. 290.

Flynn, Matthew J. "Is There a Cyber? A Review Essay," *National Cyber Security Institute Journal*, Vol. 1, No. 2 (2014): 5-8.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security*, Vol. 38, No. 2 (Fall 2013): 41-73.

Halpin, Edward. *Cyberwar, Netwar, and the Revolution in Military Affairs*. Palgrave Macmillian, 2006. Pp. 253.

Lewis, James A. "Conflict and Negotiation in Cyberspace." Center for Strategic and International Studies (CSIS), February 2013. Pp. 70.

Libicki, Martin C. "Cyberdeterrence and Cyberwar." RAND Corp, Prepared for the Air Force, 2009. Pp. 240.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013. Pp. 207.

Singer, Peter and Alan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University, 2014.

Stephenson, Scott. "The Revolution in Military Affairs: 12 Observations on an Out-of-Date Idea." *Military Review* (May-June 2010): 38-46.

US Policy in Cyberspace

Betz, David. "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed." *The Journal of Strategic Studies*, Vol. 35, No. 5 (Oct 2012): 689-711.

C*yber 2020: Asserting Global Leadership in the Cyber Domain*, Booz, Allen, Hamilton, 2010. (24)

Crosston, Matthew. "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game." *Strategic Studies Quarterly* (Winter 2012): 100-118.

Gray, Colin S. "Making Strategic Sense of Cyber Power: Why the Sky is not Falling." Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2013. Pp. 67.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security*, Vol. 38, No. 2 (Fall 2013): 7-40.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington DC: Potomac Books, 2009. Pp. 627.

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *The Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012): 401-428.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future Strategy and History*. Eds. Colin Gray and Williamson Murray. London: Frank Cass, 2004. Pp. 263.

Miller, Robert A. and Daniel T. Kuehl. "Cyberspace and the 'First Battle' in 21st-century War." *Defense Horizons*, Number 68 (September 2009), 1-6.

---------- and Irving Lachow. "Cyber War: Issue in Attack and Defense." *Joint Force Quarterly*, Issue 61, 2nd Quarter 2011: *18-23*.

Murphy, Dennis M. "Attack or Defend: Leveraging information and Balancing Risk in Cyberspace." *Military Review* (May-June 2010): 88-96.

Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Georgetown University Press, 2012. Pp. 246.

Wass de Czege, Huba. "Warfare by Internet: the Logic of Strategic Deterrence, Defense, and Attack." *Military Review* (July-August 2010): 85-96.

Cyber as a Domain

Lambeth, Benjamin S. "Airpower, Spacepowers, and Cyberpower." *Joint Force Quarterly,* Issue 60, 1st Quarter 2011: 46-53.

Lynn, William J. III. "Defending a New Domain." *Foreign Affairs*, Vol. 89, Issue 5 (Sept-Oct 2010): 97-108.

Murphy, Matt. "War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?" *The Economist*, July 1, 2010.

Stavridis, James G. and Elton C. Parker. "Sailing the Cyber Ship." *Joint Force Quarterly*, Issue 65, 2nd Quarter 2012: 61-67.

Ventre, Daniel, ed. *Cyberwar and Information Warfare*. New York: Wiley, 2011. Pp. 407.

Russo-Georgian Cyber War

"Cyber Attacks Against Georgia: Legal Lessons Identified." Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia, November 2008. Pp. 46.

Asmus, Ronald D. *A Little War That Shook the World: Georgia, Russia, and the Future of the West*. New York: Palgrave Macmillan, 2010. Pp. 272.

Hollis, David M. "Cyber War Case Study, Georgia 2008." *Small Wars Journal*. January 6, 2011. (10)

Korns, Stephen W. and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* (Winter 2008-2009): 60-76.

Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia." *Military Review* (November-December 2011): 63-68.

Russia and Estonia

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State.* Oxford: Oxford University Press, 2009. Pp. 227.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security*, Vol. 4, No. 2, Summer 2011, Strategic Security in the Cyber Age: 49-60.

Laasme, Häly. "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, Issue 63, 4th quarter 2011: 58-63.

Tikk, Eneken, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations.* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010.

China and Information Theft

"APT 1, Exposing One of China's Cyber Espionage Units." Mandiant. February 2013. Pp. 76.

Hachigian, Nina. "China's Cyber-Strategy." *Foreign Affairs* (March-April 2001), 118-133.

Krekel, Bryan, Patton Adams, and George Bakos. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage." Northrop Grumman Corp, Prepared for the US-China Economic and Security Review Commission, 7 March 2012. Pp. 137.

Lagerkvist, Johan. "New Media Entrepreneurs in China: Allies of the Party-State or Civil Society?" *Journal of International Affairs* Vol. 65, No. 1 (Fall/Winter 2011): 169-182.

Li, Zhang. "A Chinese Perspective on Cyber War." *International Review of the Red Cross*, Vol. 94, No. 886 (Summer 2012): 801-807.

Qiao, Liang and Wang Xiangsui. *Unrestricted Warfare: China's Master Plan to Destroy America*. Beijing: PLA Literature and Arts Publishing House, February 1999. Pp. 197.

Thomas, Tim L. *Decoding the Virtual Dragon.* Fort Leavenworth, KS: Foreign Military Studies Office, 2007. Pp. 352.

----------. *Dragon Bytes: Chinese Information-war Theory and Practice from 1995-2003.* Fort Leavenworth, KS: Foreign Military Studies Office, 2004. Pp. 168.

----------. "Google Confronts China's 'Three Warfares'." *Parameters* (Summer 2010): 101-113.

Just War and Cyber Conflict

Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphilian Age." *Strategic Studies Quarterly* (Spring 2011): 32-61.

Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security.* Athens, GA: University of Georgia, 2011. Pp. 331.

Cyber and International Law

"No Legal Vacuum in Cyber Space." International Committee of the Red Cross, *Resource Centre.* (2)

The Tallinn Manual. NATO, Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia. Cambridge: Cambridge University, 2013. Pp. 265.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University, 2012. Pp. 331.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs* 86:2 (2010): 523-541.

Huntley, Todd C. "Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare." *Naval Law Review*, Vol. 60 (2010): 1-40.

Philips, Kyle Genaro. "Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain." *Joint Force Quarterly*, Issue 70, 3rd Quarter 2013: 70-75.

Rustici, Ross M. "Cyberweapons: Leveling the International Playing Field." *Parameters* (Autumn 2011): 32-42.

Waxman, Matthew C. "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions." *International Law Studies*, Vol. 89 (2013): 109-122.

Stuxnet, Viruses, Malware: Guerrilla Warfare in Cyberspace

"Hacktivisim: Cyberspace has Become the New Medium for Political Voices," White Paper, McAfee, May 2012. Pp. 18.

Bowden, Mark. *Worm: The First Digital World War*. New York: Atlantic Monthly Press, 2011. Pp. 241.

Brown, Gary D. "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Force Quarterly*, Issue 63, 4th Quarter 2011: 70-73.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013): 365-404.

Metz, Steven. "The Internet, New Media, and the Evolution of Insurgency." *Parameters*, Vol. XLII, No. 3 (Autumn 2012): 80-90.

Milevski, Lucas. "Stuxnet and Strategy: a Special Operation in Cyber Space?." *Joint Force Quarterly*, Issue 63, 4th Quarter 2011: 64-69.

Shakarian, Paul. "Stuxnet: Cyber Revolution in Military Affairs." *Small Wars Journal*, April 15, 2011. (10)

Cyber as Economic Warfare. Government Protection of Critical Infrastructure

"Defining the Threat, Forging a Strategy," International Assessment and Strategy Center (IASC), Prepared for Department of Homeland Security, 30 July 2012. (62)

"In the Dark: Crucial Industries Confront Cyberattacks," Report, McAfee and CSIS, April 2011. (28)

Amoroso, Edward G. *Cyber Attacks: Protecting National Infrastructure*. Amsterdam: Elsevier, 2011. Pp. 219.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press, 2011. Pp. 319.

The Arab Spring and Social Media

"Civil Movements: The impact of Facebook and Twitter," Dubai School of Government, *Arab Social Media Report*, 1(2) (May 2011): 1-30.

"The Internet and Youth Subculture in Kuwait." In Deborah Wheeler, ed., *The Internet in the Middle East: Global Expectations and Local Imaginations in Kuwait.* Albany, NY: SUNY Press, 2006. Pp. 241. (133-162).

"New Media and Conflict after the Arab Spring," United States Institute of Peace, *Peaceworks 80* (2012): 1-24.

Alterman, Jon. "The Revolution Will Not be Tweeted." *The Washington Quarterly* 34(4) (2011): 103-116.

Anderson, Lisa. "Demystifying the Arab Spring." *Foreign Affairs*, Vol. 90, Issue 3 (May-June 2011): 2-7.

Bachrach, Judy. "Wikihistory: Did the Leaks Inspire the Arab Spring?" *World Affairs* (July/Aug 2011): 35-44.

Benon, David C. "Why the Internet Is Not Increasing Terrorism." *Security Studies* Vol. 23, No. 2 (2014): 293-328.

Bremmer, Ian. "Democracy in Cyber Space," *Foreign Affairs.* Vol. 89, Issue 6 (Nov-Dec 2010): 86-92.

Cha, Victor D. and Nicholas D. Anderson. "A North Korean Spring." *The Washington Quarterly* Vol. 35, No. 1 (2012): 7-24.

Rotberg, Robert I and Jenny C. Aker. "Mobile Phones: Uplifting Weak and Failed States." *The Washington Quarterly* Vol. 36, No. 1 (2013): 111-125.

The Warfighter in the Cyber Domain

Carafano, James J. "Mastering the Art of Wiki: Understanding Social Networking and National Security." *Joint Force Quarterly*, Issue 60, 1st Quarter 2011: 73-78.

Chondra Perry, "Social Media and the Army," *Military Review* (March-April 2010): 63-67.

Conti, Gregory. "Leadership of Cyber Warriors: Enduring Principles and New Directions." *Small Wars Journal*, July 11, 2011. (10)

----------. "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture." *Small Wars Journal*, July 29, 2010. (11)

----------. "Self-development for Cyber Warriors." *Small Wars Journal*, November 10, 2011. (34)

Crosston, Matthew. "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game." *Strategic Studies Quarterly* (Winter 2012): 100-118.

Mayfield, Thomas D. III. "A Commander's Strategy for Social Media." *Joint Force Quarterly*, Issue 60, 1st Quarter 2011: 79-83.

Cyber Deterrence

Crosston, Matthew D. "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence." *Strategic Studies Quarterly* (Spring 2011): 100-116.

Goodman, Will. "Cyber Deterrence: Tougher in Theory Than in Practice." *Strategic Studies Quarterly* (Fall 2010): 102-135.

Nye, Joseph. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 18-38.

Sterner, Eric. "Retaliatory Deterrence in Cyberspace." *Strategic Studies Quarterly* (Spring 2011): 62-80.

Stevens, Tim. "A Cyber War of Ideas: Deterrence and Norms in Cyberspace." *Contemporary Security Policy*, Vol. 33, No. 1 (April 2012): 148-170.